CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-17

Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-17 — Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur (PbMM)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte produise des spécifications de conception et une architecture de sécurité et de protection de la vie privée qui :
a. est conforme à l'architecture de sécurité et de protection de la vie privée de l'organisation qui fait partie intégrante de l'architecture d'entreprise de l'organisation
b. décrit intégralement et précisément les fonctions de sécurité et de protection de la vie privée requises ainsi que l'attribution des contrôles de sécurité parmi les composants physiques et logiques
c. expose comment les fonctions de sécurité et de protection de la vie privée, les mécanismes et les services fonctionnent ensemble pour fournir les capacités de sécurité requises et favoriser une approche coordonnée en matière de protection

Responsable : Aucun

Discussion :

L'architecture de sécurité et de protection de la vie privée et la conception des développeuses et développeurs concernent les développeuses et développeurs externes, mais elles pourraient également être appliquées au développement interne. Par opposition, le contrôle PL-08 vise d'abord les développeuses et développeurs internes de façon à ce que les organisations puissent développer une architecture de sécurité et de protection de la vie privée qui s'intègre à l'architecture d'entreprise. La distinction entre les contrôles SA-17 et PL-08 est particulièrement importante lorsque les organisations externalisent le développement des systèmes, des composants de système ou des services qui s'y rapportent et lorsqu'il est impératif de démontrer l'uniformité de l'architecture d'entreprise et celle de sécurité et de protection de la vie privée de l'organisation. Les documents 15408-2 et 15408-3 de l'ISO/IEC, et l'ITSP.10.037, Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes du CCC, fournissent de l'information sur l'architecture et la conception de la sécurité, notamment des modèles de stratégies officiels, des composants relatifs à la sécurité, de la correspondance formelle et informelle, une conception simple et la façon de structurer le droit d'accès minimal et la mise à l'essai.